# DSHS HIPAA Privacy Rule Requirement Worksheet

**1. Requirement Number: #8.12.3**

**2. Date: January 9, 2002**

**3. Originator: Marie Myerchin-Redifer**
**Title: DSHS Privacy Officer**

**4. Requirement Title: Administrative, Technical, and Physical Safeguards/Mitigation**

**5. CFR Citation: 45 CFR §164.530(c), (f) – Administrative Requirements**

**6. Requirement:** *(Provide a clear definition of the requirement as it applies to DSHS)*

**Introduction:**
A covered entity must have in place appropriate administrative, technical, and physical safeguards to prevent any intentional or unintentional violation of the privacy rule.

**Mitigation:**
If a wrongful disclosure or violation of a privacy policy is made, covered entities have a duty to mitigate any harmful effect of the violation. Such efforts may include:

- Retrieving the wrongly disclosed information,
- Preventing any future breach,
- Correcting system errors that caused the breach, and
- Educating staff on wrongful disclosure.

**Miscellaneous:**
The privacy rule does not describe particular safeguard measures because the requirements are scalable to the size of the entity. Some examples of safeguards are:

- Requiring the documents containing protected health information be shredded prior to disposal;
- Requiring that the doors to the medical records department or file cabinets be locked;
- Limiting the personnel that are authorized to have access to the PHI by requiring a key or a password.

Note: The Department of Health and Human Services (DHHS) expects safeguard requirements to work in tandem with the "minimum necessary" requirements to limit access to protected health information (PHI) by the covered entity's workforce. DHHS expects this to be a common sense scalable standard. It does not require covered entities to guarantee the safety of PHI against all assaults.

7. **Reporter:**
   **Administration/Division/Office/Program:**

8. **Date:**

9. **How do things happen now?** *(Provide a detailed description of the current policy, process and/or practice relating to this requirement. If there is none indicate that. Include system functionality if it is a part of the process or practice. Identify whether the HIPAA privacy rule preempts state law.)*

10. **Describe what needs to happen in the future:** *(This section should include a detailed description of the new or changed policies, processes or practices required to be implemented to meet the HIPAA Privacy requirements. If possible, provide detailed examples of how the change(s) will effect various case situations. This section should also include descriptions of other new/changed items such as forms, reports, interfaces, system changes, etc.)*

11. **How will this be implemented?** *(Describe implementation plans for new or change policies, processes and/or practices, including information about conversion and piloting new/changed practices and processes.)*

12. **If required changes depend upon a decision or decisions that have not been made, please specify:**

Describe the decision(s) that must be made:

When do you anticipate that his decision will be made? ___/___/___